TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 USC 371	ATTORNEY'S DOCKET NUMBER ASCOP039USNP US APPLICATION NO (if known) 09/297784

INTERNATIONAL APPLICATION NO. PCT/US97/15856	INTERNATIONAL FILING DATE NOVEMBER 7, 1997	PRIORITY DATE CLAIMED NOVEMBER 7, 1996

TITLE OF INVENTION
System for Protecting Cryptographic Processing and Memory Resources for Postal Franking Machines

APPLICANT(S) FOR DO/EO/US
G. Schwartz, et al..

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. (X) This is a **FIRST** submission of items concerning a filing under 35 USC 371.
2. ( ) This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 USC 371.
3. ( ) This express request to begin the national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 USC 371(b) and PCT Articles 22 and 39(1).
4. ( ) A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority.
5. (X) A copy of the International Application as filed (35 USC 371(c)(2)
   a. ( ) is transmitted herewith (required only if not transmitted by the International Bureau)
   b. (X) has been transmitted by the International Bureau.
   c. (X) is not required, as the application was filed with the United States Receiving Office (RO/US).
6. ( ) A translation of the International Application into English (35 USC 371(c)(2).
7. (X) Amendments to the claims of the International Application under PCT Article 19 (35 USC 371(c)(3)
   a. ( ) are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ( ) have been transmitted by the International Bureau.
   c. ( ) have not been made, however the time limit for making such amendments has NOT expired.
   d. (X) have not been made and will not be made.
8. ( ) A translation of the amendments to the claims under PCT Article 19 (35 USC 371(c)(3)).
9. ( ) An oath or declaration of the inventor(s) (35 USC 371(c)(4)). **unsigned**
10. ( ) A translation of the Annexes to the International Preliminary Examination report under PCT Article 36 (35 USC 371(c)(5).

Items 11. to 16. below concern other document(s) of information included:

11. (X) An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ( ) An Assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ( ) A FIRST preliminary amendment.
    ( ) A SECOND or SUBSEQUENT preliminary amendment.
14. ( ) A substitute specification.
15. ( ) A change or power of attorney and/or address letter.
16. ( ) Other items or information. Published PCT Application; International Search Report

US APPLICATION NO. (if known)	INTERNATIONAL APPLICATION NO. PCT/US97/15856	ATTORNEY'S DOCKET NO. ASCOP039USNP

				CALCULATIONS	PTO USE ONLY
17. (X) The following fees are submitted **Basic National Fee (37 CFR 1.492(a)(1)-(5):**					
Search Report has been prepared by EPO or JPO... $840.00					
International preliminary examination fee paid to USPTO (37CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $670.00					
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))... $760.00					
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO.. $970.00					
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4).. $ 96.00					
ENTER APPROPRIATE BASIC FEE AMOUNT =				**$ 670.00**	
Surcharge of $ 130.00 for furnishing the oath or declaration later than ( ) 20 ( ) 30 months from the earliest claimed priority date (37 CFR 1.492(e))					
Claims	Number Filed	Number Extra	Rate		
Total Claims	11 -20=	0	X $18.00	**$0**	
Independent Claims	11 - 3=	8	X $78.00	**$624.00**	
Multiple dependent claim(s) if applicable			+ $260.00		
TOTAL OF ABOVE CALCULATIONS =				**$1294.00**	
Reduction by 1/2 for filing by small entity, if applicable, Verified Small Entity Statement must also be filed. (Note 37 CFR 1.9, 1.27 and 1.28) -				**$**	
SUBTOTAL =				**$1294.00**	
Processing fee of $130.00 for furnishing English translation later than ( ) 20 ( ) 30 months from the earliest claimed priority date (37 CFR 1.492(f). +				**$**	
TOTAL NATIONAL FEE =				**$1294.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) $40 per property +				**$**	
TOTAL FEES ENCLOSED =				**$1294.00**	
				Amount to be refunded	$
				charged	$

a. (X) A check in the amount of $ 1294.00 to cover the fee above is enclosed.
b. ( ) Please charge my Deposit Account No. 15-0610 in the amount of $_________ to cover the above fees. A duplicate copy of this sheet is enclosed.
c. (X) The Commissioner is hereby authorized to charge any additional fees which may be required or credit any overpayment to Deposit Account No. 15-0610. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

Send All Correspondence To:

Oppedahl & Larson
P.O. Box 5270
Frisco, CO 80443-5270

Carl Oppedahl
Signature

Carl Oppedahl
Name
32,746
Registration Number

SYSTEM FOR PROTECTING CRYPTOGRAPHIC PROCESSING AND MEMORY RESOURCES FOR POSTAL FRANKING MACHINES

RELATED APPLICATIONS

This application claims priority from pending U.S. Provisional Application Serial Nos. 60/030,537, 60/050,043, and 60/054,105, filed on November 7, 1996, June 18, 1997, and July 29, 1997, respectively, which are hereby incorporated by reference.

TECHNICAL FIELD

This invention is directed to a system for protecting cryptographic processing and memory resources for postal franking machines.

BACKGROUND ART

In countries throughout the world, a postal customer may obtain postage from the postal authority in several ways, including the purchase of stamps and the use of a postage meter. When a postage meter is used, there is a security concern since the meter is dispensing value, and without sufficient security, the value could be stolen from a meter by unscrupulous parties. Concerns include use of the meter to dispense postage for which the Postal Authority has not been compensated and use of the meter which was not authorized by the lawful operator of the meter.

These security concerns have always been present, even when a postage meter was essentially a purely mechanical letterpress. As the postage meter evolved through the 20th century to an electronic configuration, letter-press printing was represented in a rotary drum movement impressing an image onto a mailpiece, as well as a flat-bed approach meshing a mailpiece on a platen assembly against a printing die to produce an image onto a mailpiece. The postage meter is now taking on a new role of digitally printing postage, thus no longer requiring letter-press printing.

When a postage meter utilizes letter-press printing, security concerns are typically addressed, in part, by the physical attributes of the meter. Not only do the attributes of the meter (case material, etc.) provide protection against the unauthorized use of the meter, the attributes also provide a means to detect whether an attempt has been made to make unauthorized use of the meter evidenced by visible deliberate damage to the meter's case. With evolution of the "meter," greater security against fraudulent attacks on the meter is needed. With the increase in the availability of elaborate technologies and sophisticated hacking capabilities, Postal Authorities around the world, including the United States Postal Service, are concerned with the ability to defraud the Postal Authorities by falsifying postal indicium, particularly when such indicium is digitally printed.

One approach which as been taken to increase the security of evolved meters is to employ cryptographics to the creation and application of the postal indicia. In order for this approach to be an effective security measure, however, there must be sufficient physical security for the cryptographic processing and memory to eliminate a successful fraudulent attack on the system. In order for this to be a commercially viable approach, cryptographic processing must be performed in a timely manner.

DISCLOSURE OF THE INVENTION

In accordance with the present invention, there is provided a greatly improved system for protecting cryptographic processing and memory, which also results in faster cryptographic processing. According to the invention, it is provided that the appropriate cryptographic processing and memory resources are contained in a Postal Security Device (PSD). The PSD provides physical security to these resources, thereby eliminating a successful fraudulent attack on the system. The PSD may be in the form of an Applications Specific Integrated Circuit (ASIC) and is preferably mounted on a portable device with an interface such as a Personal Computer Memory Card International Association (PCMCIA) Compliant Card or other form factor capable of supporting the integrity of the PSD.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 is a block diagram showing the basic functional makeup of the PSD cryptographic processor in the present invention.

Fig. 2 is a block diagram of the PCMCIA Card PSD of the present invention.

Fig. 3 is a block diagram showing the PSD of the present invention operating in secure high speed instruction cache operation.

MODES FOR CARRYING OUT THE INVENTION

Referring to Fig. 1, an ASIC embodiment of a PSD is shown generally at 5 and includes zeroing circuitry 10, read-only-memory 12, random-access-memory 14, switching/control logic 16, a control cryptographic processor 18, non-volatile memory 20, crypto key retention 22, signature algorithm execution 24, random number generator 26, real time clock 28, interrupt control and porting 30, clock circuit 36, secure hash acceleration circuit 44, secure memory management unit 54, and host interface 44 all within a cryptographic boundary 34. The Random Number Generator 26 within this block provides a source for non-predictable random numbers typically required in systems employing cryptographic technology. The clock circuit 28 is an on-chip realtime clock for secure time keeping. External to the ASIC PSD are a battery 32 for retaining memory contents in the absence of main power to the ASIC, and one or more crystals 37 which provide clock reference timing for the various subcircuits within the ASIC. Such a PSD contains working memory, storage memory, and firmware necessary to execute cryptographic algorithms, within its cryptographic boundary, including, but not limited to DES and RSA encryption, as well as digital signature creation and validation. Information that must be retained, as Master Key, Public Key, Private Key, and the like are secured within a non-volatile memory or battery backed up memory of the PSD. Although the battery and crystals are outside the cryptographic boundary of the ASIC in this embodiment, these components can be also integrated into the same package as the ASIC silicon die.

The ASIC provides physical security to the data stored thereon as the circuits are inaccessible without destroying circuit operation. The secure data stored on an ASIC includes data encryption keys which cannot be extracted or modified without destroying PSD operation. The encryption engine 24 includes the capability of receiving data, processing the received data by performing encryption or decryption operations.

The individual components of the ASIC may also be integrated within a PCMCIA Card, or preferably the custom integrated circuit (ASIC) is further integrated and embodied as a PCMCIA Card. The PCMCIA Card provides additional physical security through its housing for the processing unit for the storage and accounting of all funds, audit and secure support data required to produce and validate the addition and removal of postage value. As described above, one of the preferred embodiments encloses the ASIC or it components in a PCMCIA card. More generally, the invention contemplates enclosing the ASIC or its components in any package having a relatively small form factor. For example, any form factor that is more or less pocket-sized or that is more or less capable of being mailed in an envelope will be convenient. Such a package must necessarily have a communications port capable to interfacing with the postal franking device and a host, discussed below, preferably a parallel data and address bus such as is employed in a PCMCIA card. Alternatively the port could be a serial bus such as a high-speed universal serial bus. If the application does not require high speed, an infrared (LED-phototransistor) link may be used. Said secure processing unit contains working memory, storage memory, and firmware necessary to execute cryptographic algorithms, within a cryptographic boundary, including but not limited to DES and RSA, as well as digital signature creation and validation. Information which must be retained, such as Master Keys, Public Keys, Private Keys, and the like are secured within a non-volatile memory or battery backed up memory.

The security of the PSD implemented in a PCMCIA Card is a combination of data integrity, authentication, non-repudiation, and confidentiality. `Data integrity is realized through the use of cryptographic checksums (one-way hashes) over the data. This function produces a small value that uniquely represents the data, such that if any single bit is altered the hash value changes significantly. The digital signature is obtained by performing a cryptographic operation on the resultant hash of the data. Authentication is realized by the fact that the receiving party can verify the digital signature on a transmission and be assured the transmission was originated by a trusted source and not other fraudulent parties. Non-repudiation is achieved by the fact that the originator of the message cannot deny the message contents as it is possible to generate the verifiable digital signature only with the originator's unique private key. Confidentiality is the use of encryption to protect the data from unauthorized disclosure.

To ensure operational security, the PSD cannot operate as a standalone device and requires a host system to perform its functions. The PSD typically communicates directly with a host system to carry out its primary objective of indicia creation. Additionally, through the host system a user can access the PSD to review the ascending and descending register values, piece count, watchdog timeout date, and refill history logs; activate PSD diagnostics; and with proper supervisor authorization, set up and delete PINs for individual users. The PSD may also provide the user with certain operational error messages such as a low-postage warning and watchdog timeout condition through the host user interface. The host system may also maintain certain log files; these log files are required to be signed by the PSD with its private key. The host system will transfer the data to sign to the PSD and the PSD will return a digital signature and a certificate (which contains the public key which is unique to the PSD) that can be used later to verify the digital signature.

The PSD supports input and output functions with appropriate interfacing devices compatible with the PSD physical, link layer, and application protocols. Due to the secure nature of the PSD, the device does not provide user accessible diagnostic features. Rather, the PSD has an extensive built-in self test suite which is run upon power up. The tests preferably include the normal code memory verification tests, RAM tests, verification of accounting register and data log integrity, and execution of sample cryptographic calculations with known results to verify full functionality of the PSD. Upon successful completion of these tests, the PSD will be enabled to dispense postage funds. If any of the tests fail, the PSD will output its current ascending register and descending values. The host may also obtain the same information via a device audit request message. This will provide the host with additional information which may be forwarded to a Host infrastructure for the purposes of auditing the PSD. Upon the receipt and verification of a Host infrastructure-generated device audit message, preferably the PSD will reset its internal watchdog timer to accommodate control and transaction date information.

It is understood by one skilled in the art that the PSD of the present invention need not be physically located with the postal franking device; it only need be in communication with the postal franking device. For example, it may be located on the host or a computer network. In the instance of the PSD including a PCMCIA Card, the PSD may be connected to the franking device for operation and then disconnected and connected to the host for creation of the log files, etc., through a standard PCMCIA slot.

Referring now to Fig. 2, a block diagram of the embodiment of the PCMCIA Card PSD of the present invention interfacing with a host controller is shown, including host controller 64, timeout circuit 66, memory arbiter 68, controller 70, and memory 72. It is envisioned that a number of forms of attack can be executed against the PCMCIA Card PSD wherein an attacker attempts to obtain additional data from the PSD, or otherwise compromise its integrity, by holding the bus for an excessive period of time. Timeout circuit 66 operates to limit the amount of time host controller 64 may have to complete a bus transaction, and will terminate a host-initiated bus transaction if the transaction exceeds a predetermined time limit.

When host 64 wishes to access the PSD implemented in a PCMCIA Card, it waits until read signal 74 is asserted and then asserts select signal 76. This signal is input to timeout circuit 66, which initiates a predetermined timeout interval. Host controller 64 then initiates a read or write cycle by asserting the appropriate read and write signals and setting up the address and data busses accordingly.

Timeout circuit 66 provides a separate select signal 78 to memory arbiter 68, which is effectively a dual port memory controller containing logic which defines conditions under which controller 70 and host controller 64 have access to memory 72. When host controller 64 has access to memory 72, arbiter 68 asserts a hold signal 80 to controller 70, which tells controller 70 to temporarily hold off any further accesses of memory 72. Under these circumstances, controller 70 is typically idle unless it is performing an internal operation not requiring an external memory access.

Arbiter 68 allows read and write signals 82 and 84, as well as address and data busses 86 and 88, to pass onto memory 72. Following a successful bus transaction, host controller 64 deasserts select signal 74 to timeout circuit 66 to indicate the normal end of the bus transfer. Timeout circuit 66 likewise deasserts select signal 78 to arbiter 68, which removes host controller's signal levels on the read, write, address and data busses (82, 84, and 86) to memory 72 and signals the controller 70 that it can access memory 72 by deasserting hold signal 80.

If host controller 64 takes too long to complete the bus access, timeout circuit 66 deasserts ready signal 74 to the host controller and select signal 78 to arbiter 68. This causes arbiter 68 to remove host controller's 64 read (84), write (82) address (88) and data (86) signals from memory 72. Hold signal 80 to controller 70 is released to controller 70 can again access memory 72. Alternatively, timeout circuit 66 could also signal controller 70 that the fault occurred by asserting interrupt signal 90 to that device. Logic in the controller 70's software could be invoked to categorize the problem as a random fault or an attempt to compromise the PSD. If controller 70 determines tampering has been attempted, the controller would refuse further host controller 64 accesses and force the customer to report the situation to the manufacturer, for example, remotely through a telephone call or other network communication or by returning the device.

A preferred embodiment of the PSD implemented on a PCMCIA Card would restrict the area in memory 72 that host controller 64 can access. For example, access can be limited to no access, read-only, write-only, read-write, etc., and the address range in memory 72 can be restricted to a subset available to controller 70. In this manner, controller 70 can hide certain information, such as its most critical security parameters, from both observation or overwriting.

Host interface 42 incorporates timeout circuit 66, PCMCIA memory arbiter 68, and PSD controller 70. Controller 70 corresponds to crypto processor 18 in figure 1. Timeout circuit 66 and arbiter 68 would thus preferably be incorporated into the PSD ASIC but may be added as discrete circuits on the PCMCIA card.

The PSD of the present invention may be used with existing public/private key cryptographical techniques known in the art. See, for example, U.S. Patent Nos. 5,237,506, 5,606,507 and 5,666,284, which are hereby incorporated by reference. The speed with which such encryption is performed, however, may be increased by the use within the PSD of a Secure Memory Management Unit 96 (SMMU). Preferably, this is obtained from Atalla Corp., of San Jose, California, which is a Tandem Company, and VLSI Technology, of San Jose, California.

As shown in Fig. 3, Memory 98 external to the PSD contains encrypted code. SMMU 96 obtains the encrypted code 100 in portions to be processed by encryption engine 104, is such a manner that it acts as a feed for encryption engine 104. The encryption engine 104 utilizes the appropriate decryption key provided to it by the SMMU 96. This decryption key is securely stored in the PSD ASIC and is never output and so is never known to a potential attacker. The decrypted output from encryption engine 104 is then placed into RAM 106 (also 14 in Fig. 1). Fig. 3 shows the output of RAM 106 going to processor 108 (also 18 in Fig. 1). Thus, Fig. 3 depicts secure high speed instruction cache operation. The overall benefit of the SMMU is realized by the fact that a would-be attacker cannot substitute software instructions into the code to alter the intended functionality and that could give the attacker access to the master, private, or public keys held within the PSD ASIC.

While there have been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the invention and it is intended to claim all such changes and modifications as fully within the scope of the invention.

WE CLAIM:

1. A system for increasing the security and efficiency of cryptographic processing resources for postal franking machines, comprising:

(a) an encryption engine;

(b) means for obtaining encrypted code in portions to be processed by the encryption engine;

(c) random access memory;

(d) means for placing decrypted output from the encryption engine into the random access memory.

2. A method for increasing the security and efficiency of cryptographic processing resources for postal franking machines, comprising:

(a) obtaining encrypted code in portions to be processed by an encryption engine;

(b) placing decrypted output from the encryption engine into random access memory.

3. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card;

(b) means disposed within the PCMCIA Card for monitoring the amount of time a host controller is taking to complete a bus transaction;

(c) means disposed within the PCMCIA Card for comparing the monitored amount of time to a predetermined reference time;

(d) means disposed within the PCMCIA Card for refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time;

(e) an encryption engine disposed within the PCMCIA Card;

(f) means for obtaining encrypted code in portions to be processed by the encryption engine;

(g) random access memory disposed within the PCMCIA Card;

(h) means for placing decrypted output from the encryption engine into the random access memory.

4. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card;

(b) means disposed within the PCMCIA Card for monitoring the amount of time a host controller is taking to complete a bus transaction;

(c) means disposed within the PCMCIA Card for comparing the monitored amount of time to a predetermined reference time;

(d) means disposed within the PCMCIA Card for refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time.

5. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising an Application Specific Integrated

Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface.

6. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) an Application Specific Integrated Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface;

(b) said Application Specific Integrated Circuit being disposed within a Personal Computer Memory International Association card.

7. A method for protecting cryptographic processing and memory resources for postal franking machines, comprising locating the resources to be

protected within an Application Specific Integrated Circuit.

8. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card.

9. A method for protecting cryptographic processing and memory resources for postal franking machines, comprising locating the resources to be protected within a PCMCIA Card.

10. A method for protecting cryptographic processing and memory resources for postal franking machines disposed within PCMCIA Card, comprising:

(a) monitoring the amount of time a host controller is taking to complete a bus transaction;

(b) comparing the monitored amount of time to a predetermined reference time;

(c) refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time.

11. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) an Application Specific Integrated Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface;

(b) an encryption engine disposed within the PCMCIA Card;

(c) means for obtaining encrypted code in portions to be processed by the encryption engine;

(d) random access memory disposed within the PCMCIA Card;

(e) means for placing decrypted output from the encryption engine into the random access memory.

09/2 ,7184

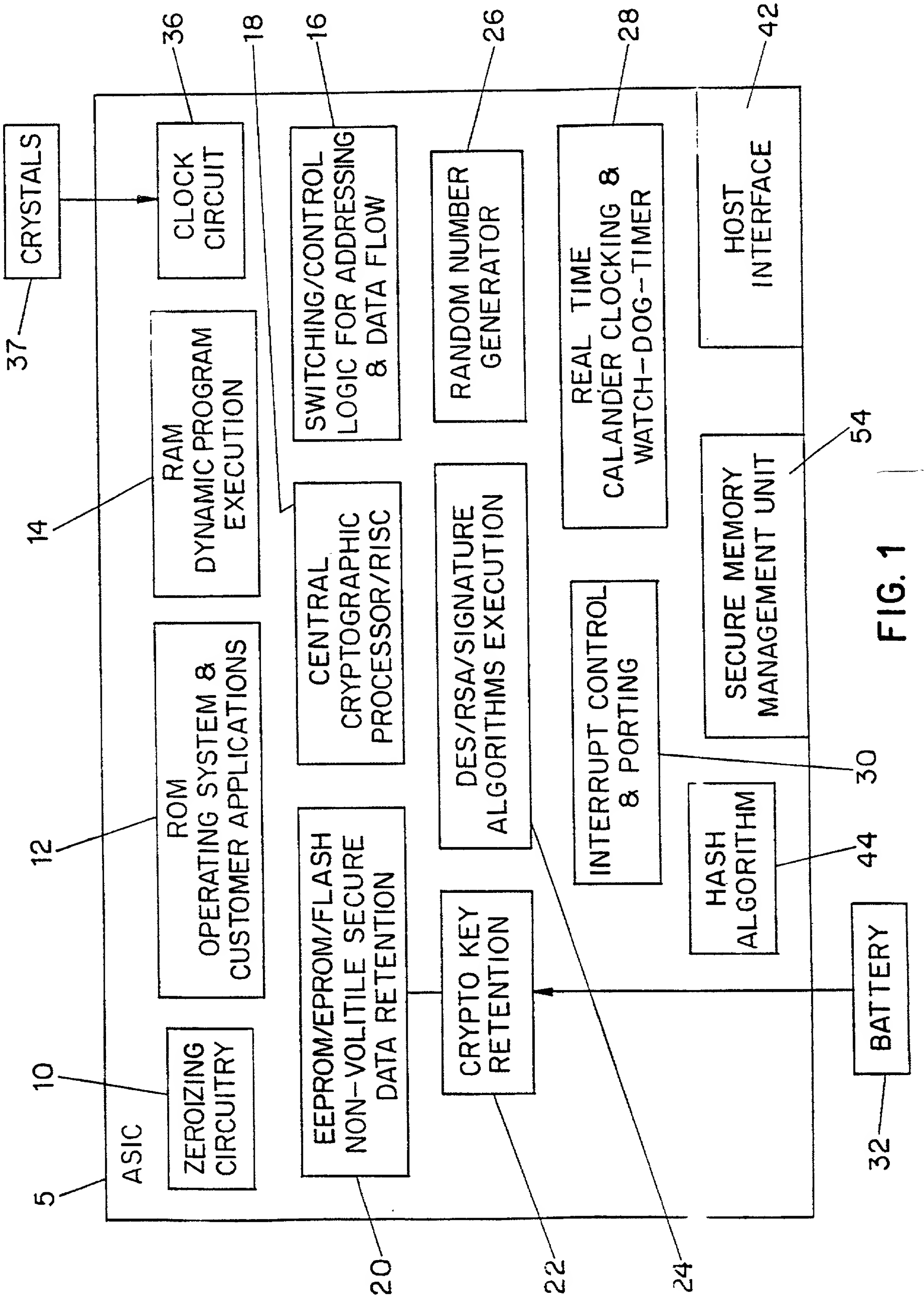
CRYSTALS
37
CLOCK CIRCUIT
36
18
16
SWITCHING/CONTROL LOGIC FOR ADDRESSING & DATA FLOW
RANDOM NUMBER GENERATOR
26
REAL TIME CALANDER CLOCKING & WATCH-DOG-TIMER
28
HOST INTERFACE
42
14
RAM DYNAMIC PROGRAM EXECUTION
CENTRAL CRYPTOGRAPHIC PROCESSOR/RISC
DES/RSA/SIGNATURE ALGORITHMS EXECUTION
INTERRUPT CONTROL & PORTING
30
SECURE MEMORY MANAGEMENT UNIT
54
12
ROM OPERATING SYSTEM & CUSTOMER APPLICATIONS
EEPROM/EPROM/FLASH NON-VOLITILE SECURE DATA RETENTION
CRYPTO KEY RETENTION
HASH ALGORITHM
44
BATTERY
32
10
ZEROIZING CIRCUITRY
ASIC
5
20
22
24

FIG. 1

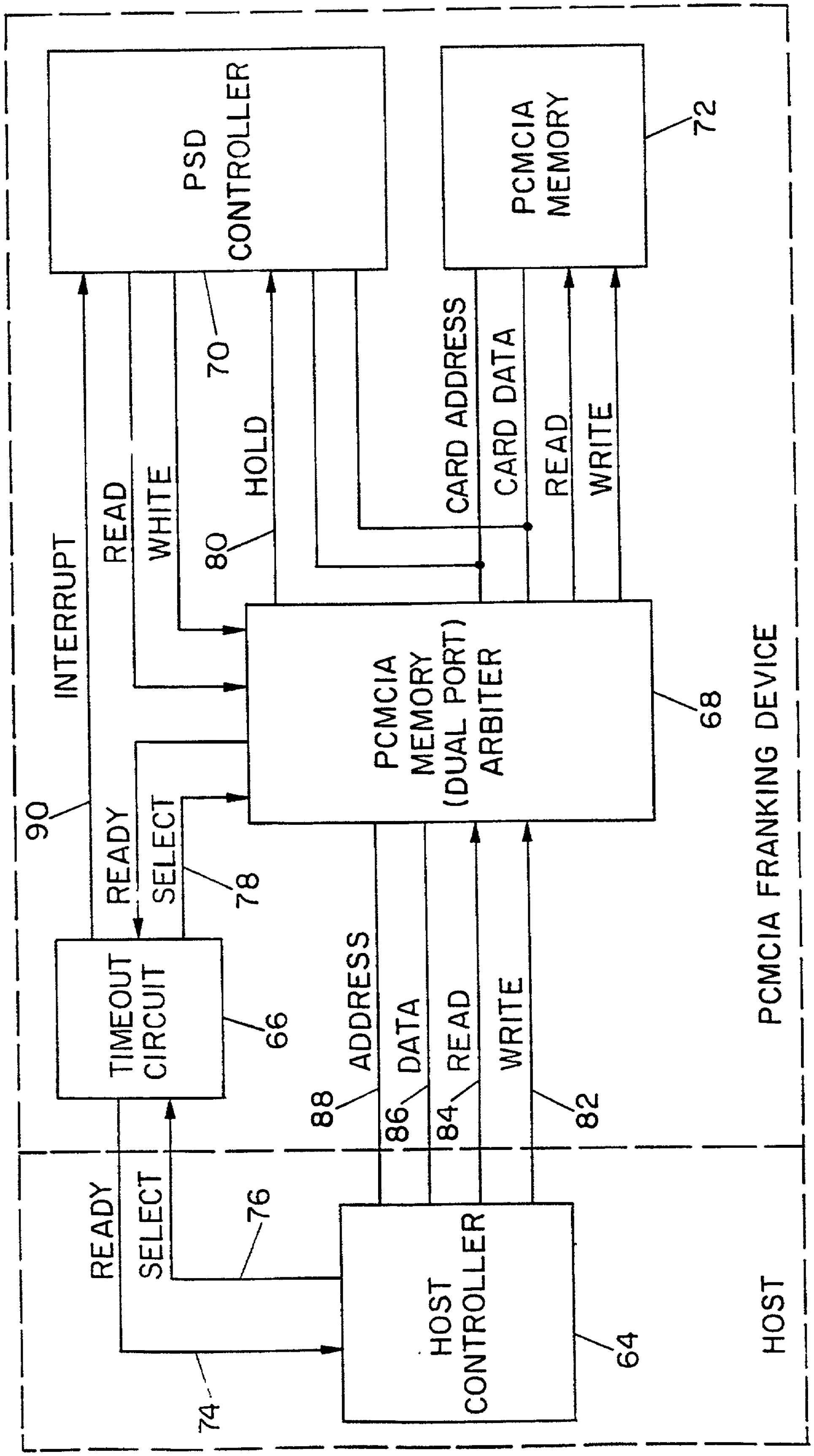
PSD
CONTROLLER
PCMCIA
MEMORY
72
INTERRUPT
READ
WHITE
80
HOLD
70
CARD ADDRESS
CARD DATA
READ
WRITE
PCMCIA
MEMORY
(DUAL PORT)
ARBITER
68
90
READY
SELECT
78
TIMEOUT
CIRCUIT
66
ADDRESS
DATA
READ
WRITE
88
86
84
82
PCMCIA FRANKING DEVICE
READY
SELECT
76
HOST
CONTROLLER
64
74
HOST

FIG. 2

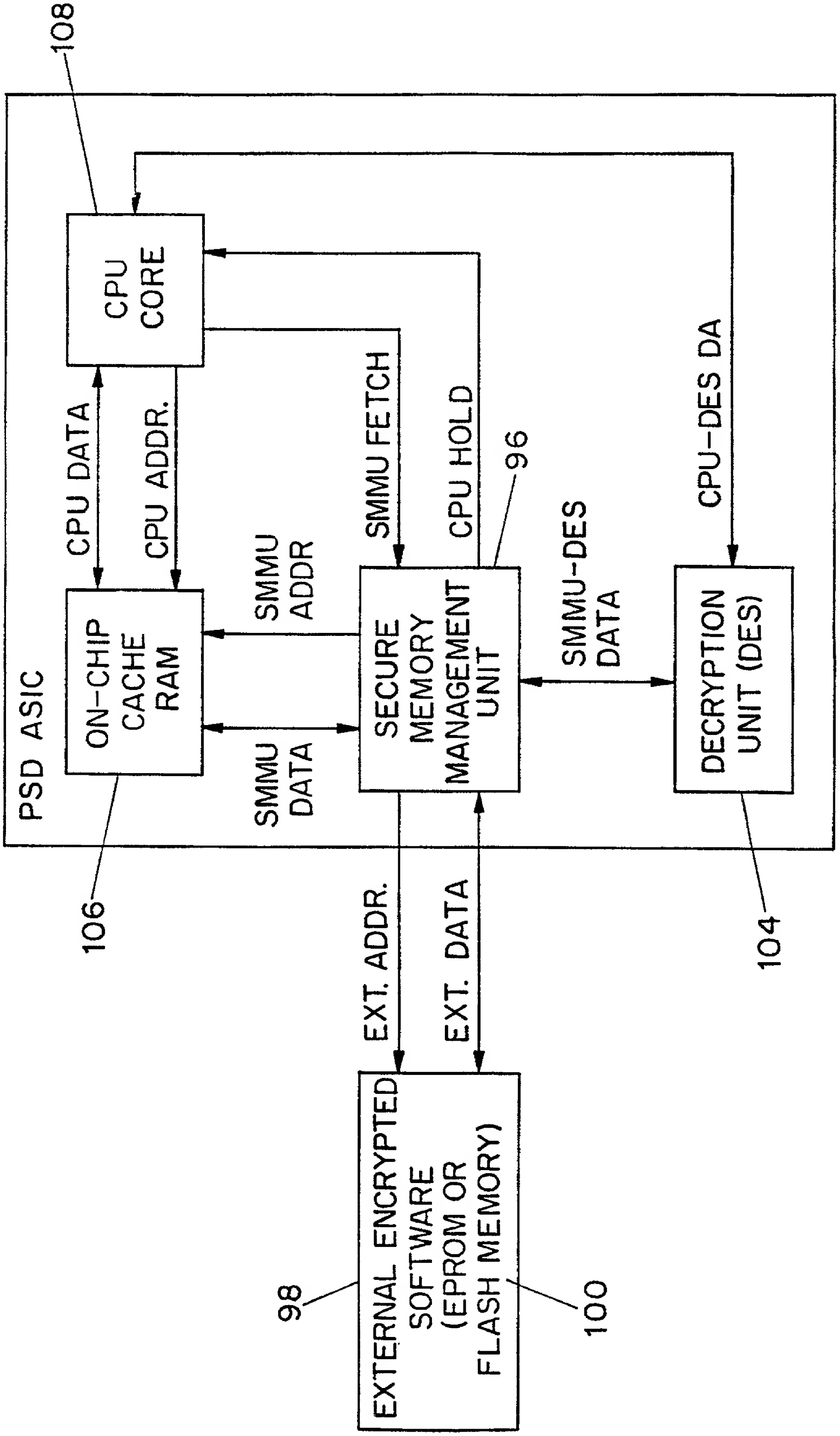
PSD ASIC
108
CPU CORE
CPU DATA
CPU ADDR.
ON-CHIP CACHE RAM
106
SMMU ADDR
SMMU DATA
SMMU FETCH
CPU HOLD
96
SECURE MEMORY MANAGEMENT UNIT
SMMU-DES DATA
CPU-DES DA
DECRYPTION UNIT (DES)
104
EXT. ADDR.
EXT. DATA
EXTERNAL ENCRYPTED SOFTWARE (EPROM OR FLASH MEMORY)
98
100

FIG. 3

Please type a plus sign (+) inside this box → ⊞

PTO/SB/01 (12-97)
Approved for use through 9/30/00 OMB 0651-0032
Patent and Trademark Office, U S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted with Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	ASCOP039
First Named Inventor	SCHWARTZ
COMPLETE IF KNOWN	
Application Number	09/297,784
Filing Date	May 07, 1999
Group Art Unit	
Examiner Name	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled.

SYSTEM FOR PROTECTING CRYPTOGRAPHIC PROCESSING AND MEMORY RESOURCES FOR POSTAL FRANKING MACHINES

(Title of the Invention)

the specification of which
☐ is attached hereto
OR
☒ was filed on (MM/DD/YYYY) 11/07/1997 as United States Application Number or PCT International Application Number US97/15856 and was amended on (MM/DD/YYYY) ________ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)
60/030/537	11/07/96
60/050/043	06/18/97
60/054/105	07/29/97

☐ Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement· This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → +

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number *(if applicable)*

□ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to tra
and Trademark Office connected therewith: ☒ Customer Number →
OR
□ Registered practitioner(s) name/registration number listed below

Name	Registration Number	Name	Number

□ Additional registered practitioner(s) named on supplemer tion sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☒ Customer Number or Bar Code Label

OR □ Correspondence address below

Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])	Family Name or Surname
ROBERT	SCHWARTZ

Inventor's Signature	Robert G. Schwartz					Date	6/23/99
Residence: City	BRANFORD	State	CT	Country	USA	Citizenship	USA
Post Office Address	191 LINDEN AVENUE						
Post Office Address	CT						
City	BRANFORD	State	CT	ZIP	06405	Country	USA

☒ Additional inventors are being named on the 1 supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto

103

Please type a plus sign (+) inside this box → +

PTO/SB/02A (3-97)
Approved for use through 9/30/98. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet Page 3 of 3

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])				Family Name or Surname			
GEORGE				BROOKNER			
Inventor's Signature	Geo Brookner					Date	22 June 1999
Residence: City	NORWALK CT	State	CT	Country	USA	Citizenship	USA
Post Office Address	11 SURREY DRIVE						
Post Office Address							
City	NORWALK	State	CT	ZIP	06851	Country	USA

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])				Family Name or Surname			
EDWARD J.				NACLERIO			
Inventor's Signature	Edward J. Naclerio					Date	6 June 1999
Residence: City	MADISON	State	CT	Country	USA	Citizenship	USA
Post Office Address	49 SCENIC ROAD						
Post Office Address							
City	MADISON CT	State	CT	ZIP	06443	Country	USA

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])				Family Name or Surname			
Inventor's Signature						Date	
Residence: City		State		Country		Citizenship	
Post Office Address							
Post Office Address							
City		State		ZIP		Country	

Burden Hour Statement: This form is estimated to take 0.4 hours to complete Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.